Cassandra Crossing/ Una nuvola in scatola

(335)— Il cloud computing è utile: utile per l'utente, ma soprattutto per chi gestisce il servizio. Per mantenere possesso e controllo sui…

Cassandra Crossing/ Una nuvola in scatola

Figure 1:

(335)— Il cloud computing è utile: utile per l'utente, ma soprattutto per chi gestisce il servizio. Per mantenere possesso e controllo sui propri dati, una ricetta per la nuvola fai da te.

12 dicembre 2014—Come molti dei 24 informati lettori avranno già capito perfettamente, l'articolo sull'hardware successore delle ormai antiche Pbox e basato su PremoBoard + Cubieboard A20 era solo la prima parte di una storia, che attende quindi il suo completamento.

Eccolo qui: ma prima, come piace tanto a Cassandra, una introduzione "storica".

Le Pbox sono state le figlie di un'epoca ormai passata, in cui alcune persone volevano una difesa "forte" della loro privacy in Rete, e talvolta anche aiutare gli altri ad averla.Questo avveniva nella Rete di oltre 10 anni fa.

Poi in Rete ci sono stati l'avvento dei servizi Google, degli smartphone con le app, di Google+, di Facebook, Twitter, WhatsApp ed infine il cloud.

Nel frattempo nel mondo si snodavano fatterelli quali Wikileaks, Collateral Murder, Cableleaks, l'esilio di Assange, la fuga di Snowden, il Datagate, le slide di Greenwald con l'elenco delle aziende cooptate dall'NSA…

I fatterelli non hanno tuttavia influenzato molto le abitudini dei più.

Si, la Merkel si è arrabbiata ed ha cambiato telefono, Apple ha modificato le policy di backup e restore, tanto care a guardoni normali e di tre lettere, giornali e talk show hanno avuto un argomento ganzo e tecnologico con cui riempire pagine e palinsesti per mesi.

Cambiamenti, però, ce ne sono stati solo nell'industria, negli investimenti in cyberwarfare e nella geopolitica della Rete.

Al contrario, le abitudini deleterie, anzi suicide, per la privacy delle persone non sono cambiate, e nessuno è sceso in piazza per protestare contro il tecnocontrollo.

Una battaglia è finita ed i "buoni" ("buoni" secondo Cassandra, ovviamente) hanno perso, anzi si sono arresi senza opporre resistenza.È ora di guardare alla sfida successiva.

Il Cloud, anzi la "cloudificazione" di tutti i dati, è probabilmente l'argomento più importante. L'accesso ai dati è come l'acqua per la vita: è indispensabile.

Ma l'acqua non è la vita, la rende solo possibile: i dati sono la vita.

Se non potete copiare i dati, ma solo accedervi tramite i servizi, i dati non sono vostri.

Se i dati non sono disseminati, ma concentrati in grandi archivi, non sono di tutti. Ciò che è centralizzato e richiede risorse per essere utilizzato non è libero.

Ecco perché considerare di avere accesso alla cultura solo perché si possiede un link per arrivarci è fondamentalmente errato. Il link cessa di funzionare (o visualizza la richiesta di una carta di credito) ed i dati che credevate liberi sono spariti.

È successo con le terre pubbliche (i "commons"), secoli fa in Inghilterra, sta succedendo oggi con i dati pubblici in Rete.

Ma questo si è capito? Mica tanto, pare…I dati personali, generati dagli individui e che prima risiedevano sui pc, sui portatili e sugli smartphone, ora vengono copiati e spesso memorizzati in "nuvole" fornite gratis o quasi da sorridenti Mangiafuoco. Così anche i dati prodotti da noi non sono più in nostro possesso."

"*Ma sono nel Cloud*—potrebbe obiettare qualcuno—*è come se fossero miei e sui miei device, visto che li posso raggiungere quando voglio: anzi, sono anche più al sicuro*".

No, non è così: se avete bisogno di qualcun altro per accedere ai vostri dati, se altri ci possono fare quello che vogliono, se accedervi richiede servizi gestiti da altri, bene, reggetevi forte, voi non solo avete regalato i vostri dati ad altri, ma non li avete nemmeno più. Potete accedervi se, come e quando vi viene permesso.

Tutte le tirannie cominciano come utopie.

Tutte le fregature sembrano belle, all'inizio."*Eh mannaggia, quanto siamo andati lontano!*" bofonchieranno alcuni dei 24 impazienti lettori.

Per andare sul pratico e riciclare quanto fatto in passato, ora che sappiamo che il Cloud è bello ma pericoloso, chiediamoci: possiamo farne a meno ed averlo nello stesso tempo?

Certo, basta avere la Pbox modello V la Cloud-in-a-Box.

Farsi in casa il proprio Cloud, condividerlo con persone selezionate, amici, colleghi e parenti.

Spendere qualche soldo e fare a meno di qualche servizio gratuito. Avere il Cloud, ma anche il possesso dei propri dati.

Non "il controllo", proprio "il possesso".

Farsi le cose a casa ed in maniera semplice, proprio come ai tempi delle Pbox, ma per un'applicazione completamente diversa.

Chiamiamola una nuvola privata, una nuvoletta in scatola.

Chiamiamola appunto Cloud-in-a-Box.Ecco una ricetta semplice.

Primo, prendete un oggetto che riesca a girare un sistema operativo serio come Debian, ma anche un'altra versione di GNU/Linux, ma anche un windows*.

Se volete costruirvi una nuvola personale vi consiglio un hardware come quello illustrato nel precedente articolo. La versione con Cubie A20+ PremoBoard + HDU da 500 GB, grazie alle due antenne wireless può anche collegarsi alla vostra ADSL WiFi con una e fare da access point con l'altra, creando una nuvoletta privata WiFi con accesso diretto alla nuvola.

Figure 2:

Secondo, installate ownCloud 7.0: Owncloud ha una versione Enterprise, ma quella Community ci basta ed avanza.

Selezionate la piattaforma ed il sistema operativo che volete usare, scaricate il software opportuno ed installatelo. Considerate che si tratta di una applicazione LAMP, Linux, Apache, Mysql e PHP.

Potete sostituire Linux e MySQL con un altro sistema operativo ed un altro database, ma Apache e PHP li dovete installare.

Niente paura, però, è un lavoro semplice: convincersi di dover prendere in mano almeno una piccola parte del proprio destino è la cosa più difficile. Attivate la crittografia, settatelo per usare solo https, collegatevi come admin, attivate le applicazioni che volete (la crittografia è disattiva per default), definite utenti, gruppi e quote.

Ora i vostri nuovi utenti potranno collegarsi via https o webDAV, utilizzando browser...
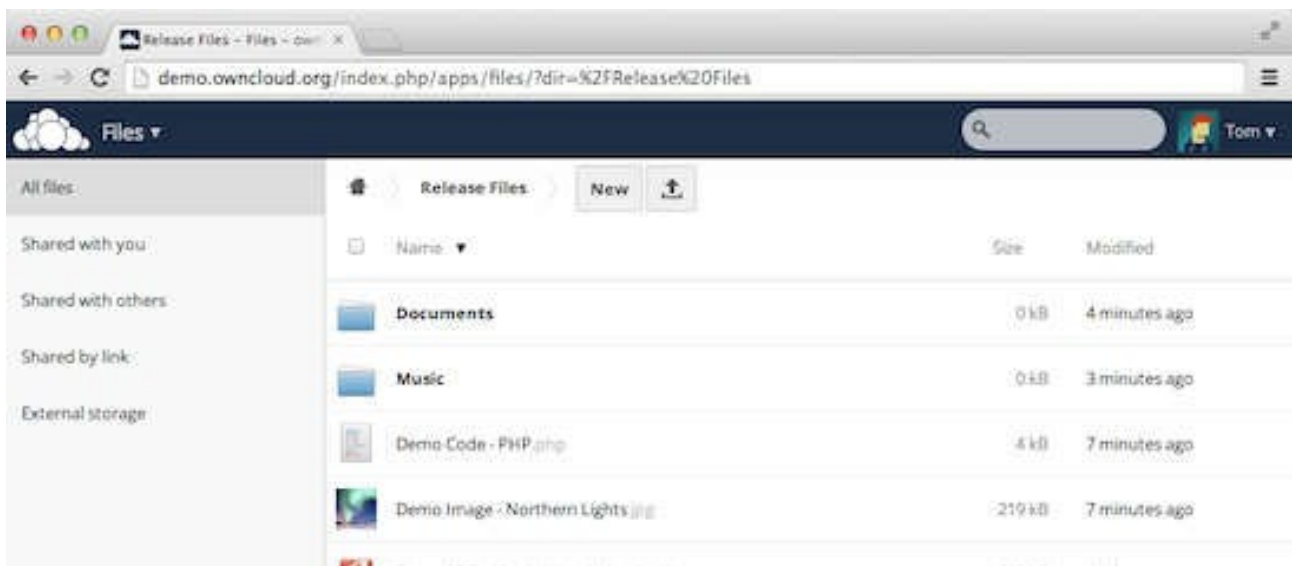
Figure 3:

...client in background...
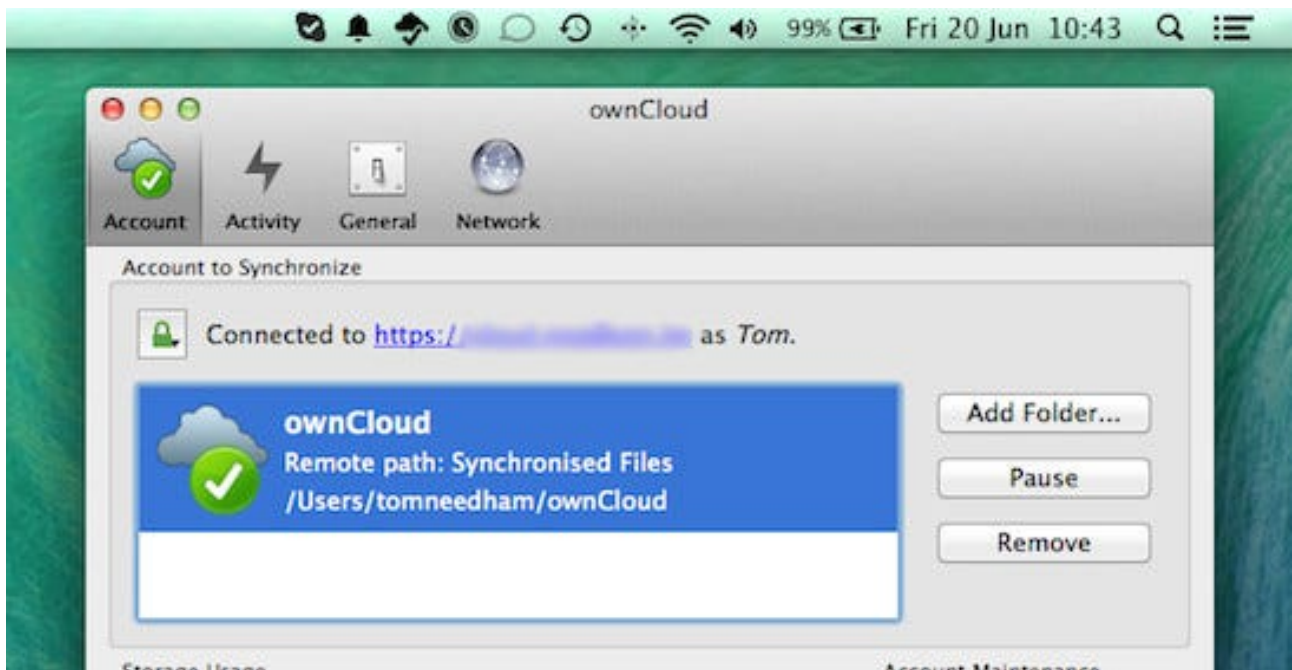
Figure 4:

...o anche una app dedicata.
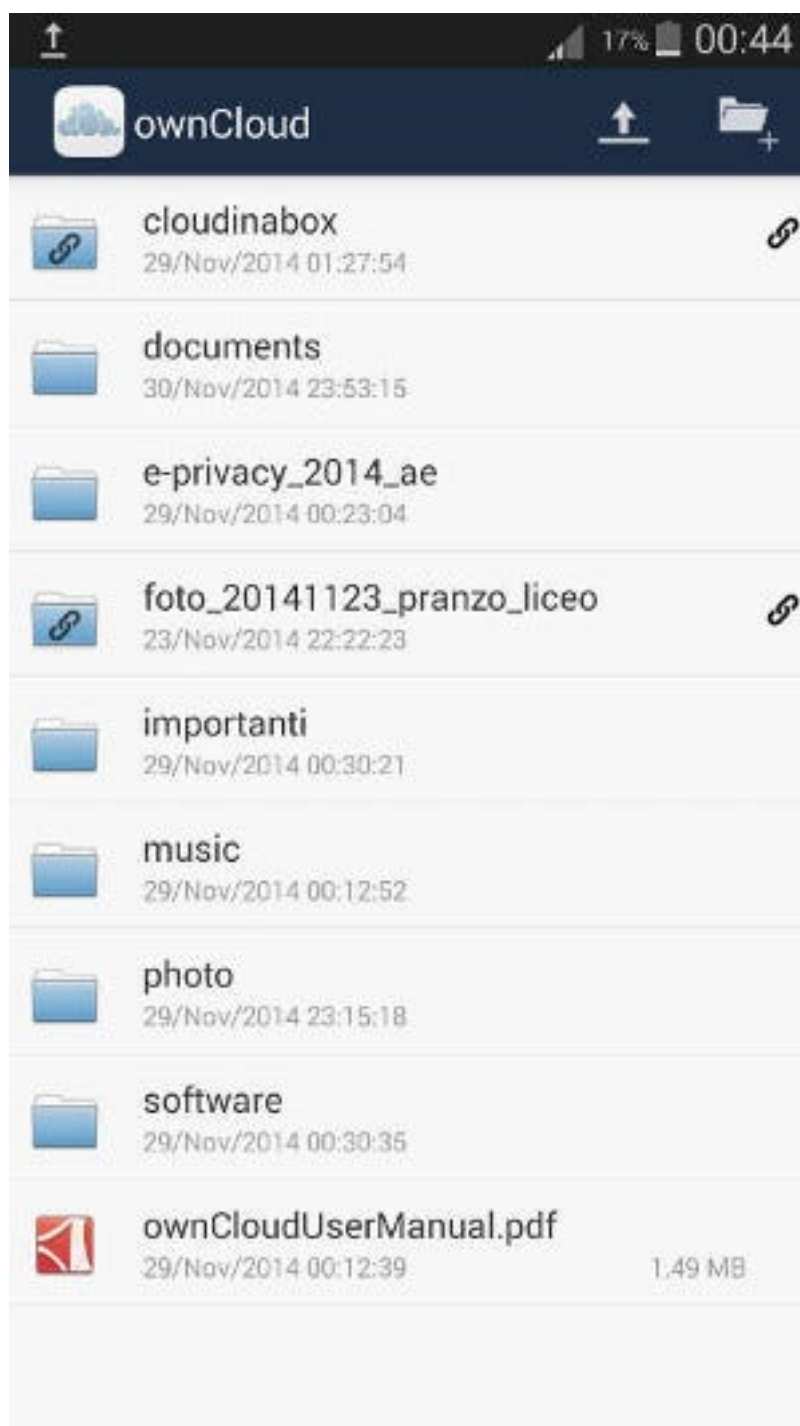
Figure 5:

In quest'ultimo caso, se scaricate la app di ownCloud dal Play Store si tratterà di una applicazione a pagamento, il che significa non tanto pagare 80 centesimi, ma dover creare un account MyWallet contenente i dati della vostra carta di credito e che può essere usato (se non state attenti) anche per comprare altre app o per comprare contenuti dall'interno di app).

Molto meglio installarsi il repository alternativo F-Droid, e da lì scaricare la versione libera dell'app. Usate i link forniti direttamente sul sito di ownCloud.

Infatti è importante sapere che F-Droid è uno store di applicazioni sotto licenza libera, ma se bisogna sempre fare attenzione a cosa si scarica: in un contesto meno controllato di uno store commerciale bisogna farlo ancora di più, poiché anche un virus o un malware possono essere

sotto licenza libera.

Da questo momento potete uploadare e downloadare via browser o via client dalla vostra nuvola privata, potete sincronizzare automaticamente directory, potete sincronizzare i vostri bookmark e/o contatti (quest'ultima cosa con qualche limitazione a seconda delle caratteristiche software del vostro device).

Avrete anche a disposizione le stesse funzionalità fornite dal più famoso (e commerciale) DropBox. È possibile pubblicare un singolo file o un folder, accessibile con un link che richiede se necessario anche una password, diversa da quella del vostro account, e se necessario dotata di scadenza.È possibile abilitare un folder pubblicato al solo download o anche all'upload di file, sempre con link e password create ad hoc e strettamente limitate.

Per quanto riguarda sicurezza e crittografia, la sicurezza deriva innanzitutto dal fatto che l'hardware è vostro, sta a casa vostra su un aggeggio piccolo, che consuma poco e trova spazio in un cassetto o su un mobile.

La crittografia utilizzata è di un modello elementare, niente crittografia client side, perciò: la sicurezza dei vostri dati è garantita durante il transito dal protocollo https, e quando sono scritti sullo storage da crittografia. Le chiavi sono però sul server, e sono bloccate dalla vostra password.

Il sysadmin o chi venisse in possesso del disco non potranno quindi risalire al contenuto dei vostri file (ai nomi sì), ovviamente se avete scelto una password robusta e l'avete custodita ed utilizzata con cura.

ownCloud non è perfetto: è solo molto, molto meglio che utilizzare i servizi commerciali.

Perché è vostro. Enjoy.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on November 16, 2023.

Canonical link

Exported from Medium on August 27, 2025.